ID: 562520
Sample Name:
qpwx2wT5ky.exe
Cookbook: default.jbs
Time: 00:10:16
Date: 29/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

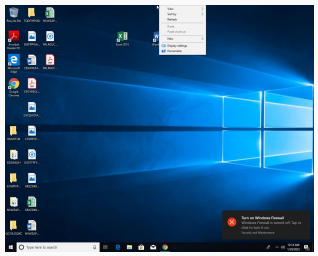
Windows Analysis Report

qpwx2wT5ky.exe

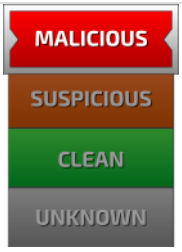
Overview

General Information

Sample Name:	qpwx2wT5ky.exe
Analysis ID:	562520
MD5:	c22c0fdbc19dcd…
SHA1:	4cd9280315ce4f…
SHA256:	d72ff8708ffeb9a…
Tags:	exe RaccoonStealer
Infos:	



Detection



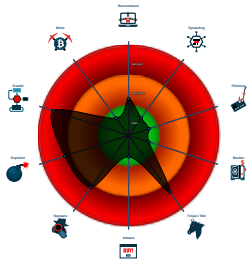
Raccoon

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e…
- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected Raccoon Stealer
- Antivirus detection for URL or domain
- Writes to foreign memory regions
- .NET source code references suspic…
- Contains functionality to hide user a…
- Tries to detect sandboxes and other…
- Contains functionality to steal Intern…

Classification



Process Tree

- **System is w10x64**
- qpwx2wT5ky.exe (PID: 6428 cmdline: "C:\Users\user\Desktop\qpwx2wT5ky.exe" MD5: C22C0FDBC19DCD4838709BBACA921F56)
  - LaunchWinApp.exe (PID: 5980 cmdline: C:\Windows\SysWOW64\LaunchWinApp.exe MD5: 529B7E6E938EA6C3BCA2821EB525BBD7)
    - WerFault.exe (PID: 5952 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5980 -s 796 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Raccoon Stealer


```
{
  "RC4_key2": "5611095ee49218feb5b751c501370b8c",
  "C2 url": [
    "http://188.166.1.115/hdm3prapor",
    "http://91.219.236.139/hdm3prapor",
    "http://194.180.174.147/hdm3prapor",
    "http://185.3.95.153/hdm3prapor",
    "http://185.163.204.22/hdm3prapor",
    "https://t.me/hdm3prapor"
  ],
  "Bot ID": "79e83b057f17f4dd954bc4809f7290094846fc1f",
  "RC4_key1": "jY1aN3zZ2j"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.318536230.0000000004271000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
00000000.00000002.318536230.0000000004271000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
00000002.00000000.308435428.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
00000002.00000000.308435428.0000000000400000.00000040.00000400.00020000.00000000.sdmp	MALWARE_Win_Raccoon	Raccoon stealer payload	ditekSHen	• 0x7e47c:$s1: inetcomm server passwords • 0x86f44:$s4: CredEnumerateW • 0x7e048:$s5: %[^:]://%[^/]%[^ • 0x7e064:$s6: %99[^:]://%99[^/]%99[^ • 0x7b050:$s8: m_it.object_iterator != m_object->m_value.object->end() • 0x7d728:$x1: endptr == token_buffer.data() + token_buffer.size() • 0x7d0e8:$x2: \json.hpp • 0x7da34:$x3: Microsoft_WinInet_ • 0x7db44:$x3: Microsoft_WinInet_ • 0x7db44:$x4: Microsoft_WinInet_*
00000002.00000002.503612673.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.qpwx2wT5ky.exe.46615d0.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.3.qpwx2wT5ky.exe.46615d0.1.raw.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
0.3.qpwx2wT5ky.exe.46615d0.1.raw.unpack	INDICATOR_SUSPICIOUS_DisableWinDefender	Detects executables containing artifcats associated with disabling Widnows Defender	ditekSHen	• 0x8ee04:$e1: Microsoft\Windows Defender\Exclusions\Paths • 0x8ee60:$e2: Add-MpPreference -ExclusionPath
0.3.qpwx2wT5ky.exe.46615d0.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCMD	Detects Windows exceutables bypassing UAC using CMSTP utility, command line and INF	ditekSHen	• 0x903e3:$s1: c:\windows\system32\cmstp.exe • 0x9017f:$s2: taskkill /IM cmstp.exe /F • 0x9003b:$s5: RunPreSetupCommands=RunPreSetupCommandsSection • 0x90271:$s6: "HKLM", "SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\CMMGR32.EXE", "ProfileInstallPath", "%UnexpectedError%", ""
0.3.qpwx2wT5ky.exe.46615d0.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM	Detects executables embedding command execution via IExecuteCommand COM object	ditekSHen	• 0x8ebd2:$r1: Classes\Folder\shell\open\command • 0x8ec16:$k1: DelegateExecute • 0x8ead2:$s1: /EXEFilename "{0} • 0x8eaf8:$s2: /WindowState "" • 0x904e6:$s2: /WindowState "" • 0x8eb22:$s3: /PriorityClass ""32"" /CommandLine " • 0x9050c:$s3: /PriorityClass ""32"" /CommandLine " • 0x8eb6e:$s4: /StartDirectory " • 0x90558:$s4: /StartDirectory " • 0x8eb94:$s5: /RunAs • 0x9057e:$s5: /RunAs
Click to see the 77 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Multi AV Scanner detection for submitted file

Yara detected Raccoon Stealer

Antivirus detection for URL or domain

Exploits

Yara detected UAC Bypass using CMSTP

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Raccoon Stealer

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection

Contains functionality to hide user accounts

Moves itself to temp directory

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Raccoon Stealer

Contains functionality to steal Internet Explorer form passwords

Remote Access Functionality

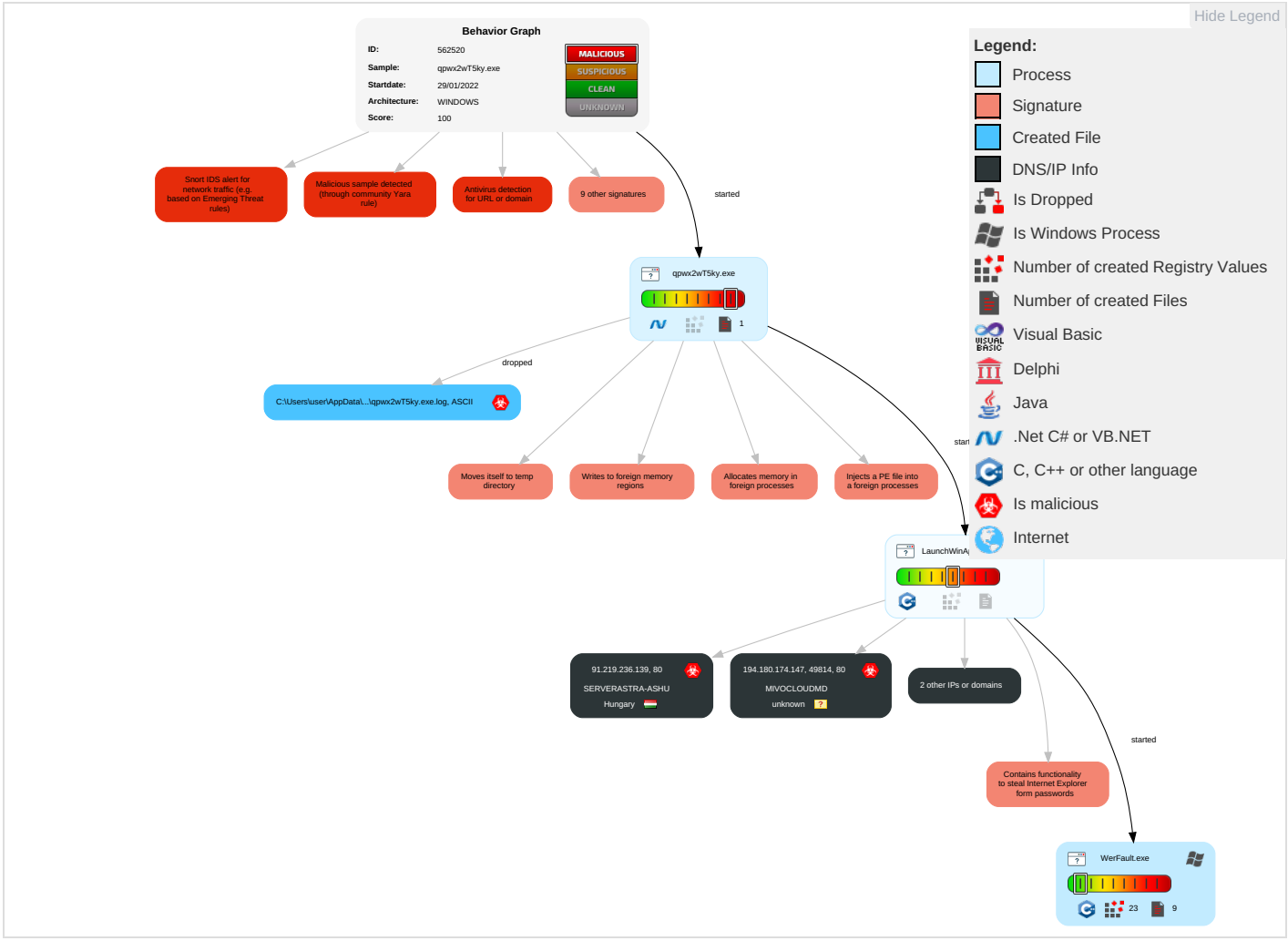
Yara detected Raccoon Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Native API	Path Interception	3 1 1 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	1 Credentials In Files	1 Account Discovery	Remote Desktop Protocol	1 Screen Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Software Packing	NTDS	3 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Masquerading	LSA Secrets	1 4 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 1 1 Process Injection	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Users	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

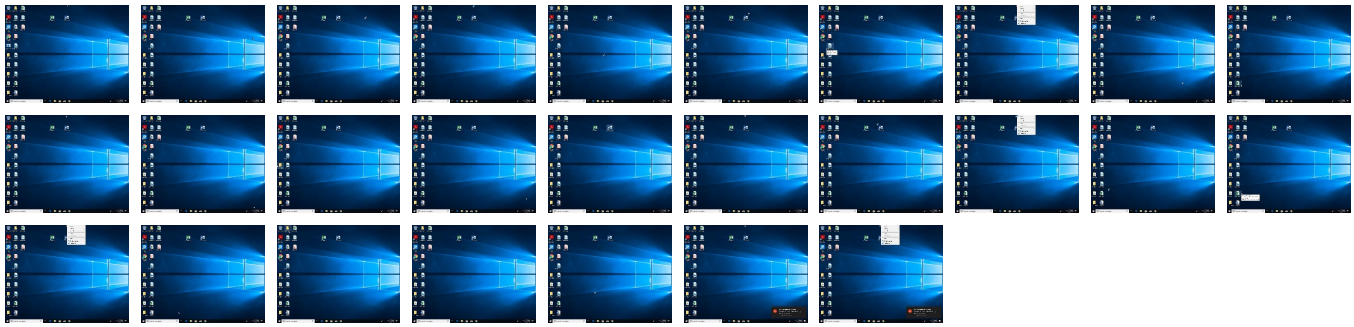
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
qpwx2wT5ky.exe	48%	Virustotal		Browse
qpwx2wT5ky.exe	24%	Metadefender		Browse
qpwx2wT5ky.exe	67%	ReversingLabs	ByteCode-MSIL.Infostealer.Racealer	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.LaunchWinApp.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1143241		Download File
2.0.LaunchWinApp.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1143241		Download File
2.0.LaunchWinApp.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1143241		Download File
2.0.LaunchWinApp.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1143241		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.LaunchWinApp.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1143241		Download File
2.0.LaunchWinApp.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1143241		Download File
2.0.LaunchWinApp.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1143241		Download File
2.0.LaunchWinApp.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1143241		Download File
2.0.LaunchWinApp.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1143241		Download File
2.0.LaunchWinApp.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1143241		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://91.219.236.139/hdm3prapor	2%	Virustotal		Browse
http://91.219.236.139/hdm3prapor	0%	Avira URL Cloud	safe	
http://185.163.204.22/hdm3prapor	100%	Avira URL Cloud	malware	
http://194.180.174.147/hdm3prapor	1%	Virustotal		Browse
http://194.180.174.147/hdm3prapor	0%	Avira URL Cloud	safe	
http://185.3.95.153/hdm3prapor	0%	Avira URL Cloud	safe	
http://159.223.25.220/	0%	Avira URL Cloud	safe	
http://188.166.1.115/hdm3prapor	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

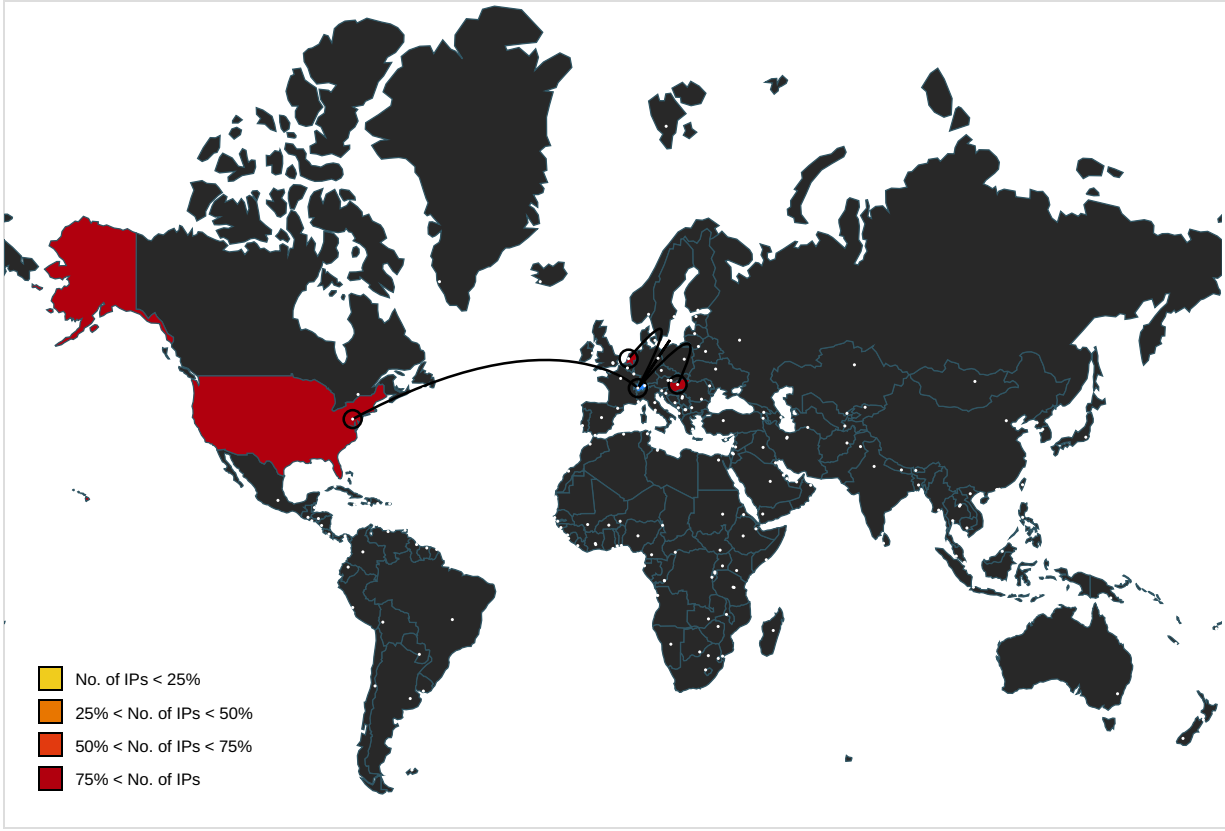
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://91.219.236.139/hdm3prapor	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.163.204.22/hdm3prapor	true	• Avira URL Cloud: malware	unknown
http://194.180.174.147/hdm3prapor	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.3.95.153/hdm3prapor	true	• Avira URL Cloud: safe	unknown
http://159.223.25.220/	false	• Avira URL Cloud: safe	unknown
http://https://t.me/hdm3prapor	false		high
http://188.166.1.115/hdm3prapor	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://upx.sf.net	Amcache.hve.16.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.166.1.115	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
159.223.25.220	unknown	United States		46118	CELANESE-US	false
194.180.174.147	unknown	unknown		39798	MIVOCLOUDMD	true
91.219.236.139	unknown	Hungary		56322	SERVERASTRA-ASHU	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562520
Start date:	29.01.2022
Start time:	00:10:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qpwx2wT5ky.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winEXE@4/7@0/4

EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.182.143.212
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, onedsblobprdcus15.centralus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
00:12:47	API Interceptor	5x Sleep call for process: LaunchWinApp.exe modified
00:13:44	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LaunchWinApp.exe_774587b722d421177778692fbd3ea27ebb729dee_d75afd38_16ec8da7\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9168915727727842

Encrypted:	false
SSDEEP:	192:29rIDKfGGcHRUEMm2Fj2K/lg/u7seS274Ita:qrIgkRUEMmCjG/u7seX4Ita
MD5:	704712E4245884343C1B53D933E0FF6A
SHA1:	735EC03A19C628348BA75BED82093B1B0CE7A212
SHA-256:	0E75A303D3BCF10BF5A5769CFF6CB03ADF0D7C65B06302790B3033433224CDC5
SHA-512:	995834F87714AC2E91235362A2DA6B33CCEC59871C52771C3F85AC3545FB90CE19C58F4666BB58C476F52541FF5F0E04038E8C5B087271B747C6F342382F1146
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.7.9.1.7.6.1.3.5.6.7.3.8.3.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.7.9.1.7.6.2.2.6.2.9.8.2.1.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.0.9.6.4.0.7.2.-.a.9.2.9.-.4.4.8.c.-.8.a.6.1.-.c.d.b.9.8.a.6.4.8.8.c.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.e.8.5.8.a.7.7.-.e.2.8.c.-.4.0.0.0.-.8.9.6.b.-.9.d.a.4.9.6.7.6.c.4.2.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.L.a.u.n.c.h.W.i.n.A.p.p...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.L.a.u.n.c.h.W.i.n.A.p.p...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.5.c.-.0.0.0.1.-.0.0.1.c.-.5.0.6.c.-.1.4.e.c.e.7.1.4.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.0.b.3.9.e.6.e.0.9.8.0.6.7.f.0.a.f.8.5.d.3.6.1.d.5.1.0.7.a.b.2.2.4.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8358
Entropy (8bit):	3.6892430773725198
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNip/p6Nm6Yyj61ugmf8EeS/ENrCpD589b7hsfPJm:RrlsNipB6c6YO6sgmf8EeS/EH7afM
MD5:	DB040076D87CFF2B5E68679D4C1ED53F
SHA1:	66CFADBBF5D16B035B0C6215E2CAAF02A43017DD
SHA-256:	833EAB64A8B988574F0F3A7AD22F53D47CBE0EAB44B9A3E962EA9D4280202B8F
SHA-512:	AA989CFA5D089DBE760C91EA5BAEFD952AAFF4CAB1D813C6FB77AE47A7B3F3FBC3F6F94D77FFA7271C3F784F0C17BA4E2D3D33B1ABF0A126966BF8E0A33D3499
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.9.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C6.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4768
Entropy (8bit):	4.461867495702939
Encrypted:	false
SSDEEP:	48:cvIwSD8zshJgtWI9HXWSC8BzM8fm8M4JRpigWcItFvx+q8vWigWcITDXGnMPrIPe:ulTfzkmSNXJARKN32orchad
MD5:	D1AF0BA5079F3DE14DD7E8051DFB5C05
SHA1:	97CC0473AD86735F7F628D6888D4D956CE106184
SHA-256:	D0C5DD19873B1D9B87B8571680CD3F82DA7FCF7B31DBCC54CB35C764ECAD1B9A
SHA-512:	DBF3ABFC6C8DDE6CBCC5EABDBA57C426C30D611DD5E209E15CA83C724501248E2E5E7466E2F5295B1FEA7B0F50F7AA8868C6BEA634469CD740AEF8C1ED5ADC32
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1363284" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Jan 29 08:13:37 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	61158

Entropy (8bit):	2.4767519839533017
Encrypted:	false
SSDEEP:	192:3KmU3CNYulpOCzAoVE/tsu25X0mAJZ8QXqk7xtebbqn10RWWeOAuZ+5ZHTUnDaBC:fSisC8r0+mAJZ8axt2vABsG4FmA
MD5:	416A11DCE14D66C77506CE1A74542009
SHA1:	DEA54DFEEF7500324613857BE92392FA40A61202
SHA-256:	69AF6348A49402738E7EE52678C15E76C67FA123319B11CF32DED5509A324434
SHA-512:	E541F05F091B39FBA805B22ED62E172988575D02F4225BB8D86A1A0DD15C344D2454AF4D57A905C85F6A54657C2555EA9545AD6396A4C763BC01257D31971277
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....1..a.....(.....0.....`.....8.....T..... .....p.....U.....B..... ...GenuineIntelW.....T.....\.....a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\qpwx2wT5ky.exe.log

Process:	C:\Users\user\Desktop\qpwx2wT5ky.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	5.347480285514745
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat92n4M0kvoDLI4MWuCv:ML9E4Ks2wKDE4KhK3VZ9pKhg84jE4Ks
MD5:	C090C3A5090FDB569FD50003722EDAD4
SHA1:	878B12213721F0ED188986C03408AEFBD2F0D1AE
SHA-256:	3D04A30D0B4C7F044488F425F4BBC78573B5AB98B9586A9C99D3760E11ED4955
SHA-512:	157F60DD6B99B500694DFB13A3186E3F253468E03DED8075B9671337E51E89A208FA35E9263B2C0F6460205FEE89481C8EE36FD7BBCE66BB399F1D27BDF82609
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Windows\appcompat\Programs\Amcache.hve

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.2740946580710055
Encrypted:	false
SSDEEP:	12288:f+ty5r16YgMk9OszLl2/n1dRQAK7WN+A2wo5lKe85v5tk0GHezT/V:Gty5r16YgMk9OsCd
MD5:	8CE94B0FFC9D2328821B50E5A619DD53
SHA1:	5F11244FC9C2919CD1E345339803F44F06F0EEAF
SHA-256:	FD946DB2798FB9ACA18A737898A1CA66C1BA34B9C6AD92FB637CA39822D6B6E5
SHA-512:	C94F74438963710015DC1CABF57D0E5888EEFC29264EA402DEBD0B4E3AB2245B66E22D0B7295BB7F01A52DAA42F518212C94555344F899C4BEDC732E27FB300D
Malicious:	false
Reputation:	low
Preview:	regfZ...Z...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E....5.....E.rmtm..... ....D..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	4.031260608135238
Encrypted:	false

SSDEEP:	384:5r6l5Rftx1HPJ4XYs1Fn87kkPBqXXSeq5QMVyiy+/ql4Lk4jZd1DoXznH7tNAG:56bRftx1vJ4X91F87hBqXCeq5QMVyiyY
MD5:	216E7FDAF7B821B8B2C10D83992D0236
SHA1:	9FDF64BF1DE8E4F7493FBBD25268F6320306BFD1
SHA-256:	218E0B0C02C620819688CA35F8A0A43A10B1424BE922FF80F26A6666976977ED
SHA-512:	5965CC1C9BED17338D274BAECC6282F7B4687223B4F79B5944EDCE537AFB81F4C386FCB79665B2AEC9D358A486511E67263F30AD14604150AE5D39D24DF6DEB
Malicious:	false
Reputation:	low
Preview:	regfY...Y...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..... ....DHvLE.^.....Y.....r|..z];..u.vr.....0..... ..hbin.....p.\..,.....nk,.Pe..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .Pe..... ....Z.....Root.....lf.....Root....nk .Pe.....}..... .....*.....DeviceCensus..... ..vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.393740189625997
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	qpwx2wT5ky.exe
File size:	1128960
MD5:	c22c0fdbc19dcd4838709bbaca921f56
SHA1:	4cd9280315ce4ff97cdb95d7dd6d8fcb7715f292
SHA256:	d72ff8708ffeb9a95f559828938dc1439884e7c224579127418e285b1aa1d235
SHA512:	207be844380090fdb580bf006dab730643abd4b5a1fafd6d847a2f0831b412294d303399dd23baaf60b47660f326633544fd31ac893acd697bb531767e085943
SSDEEP:	24576:MeMhSdxLmSbEoA7El4dwcfrQRqXRJ6XjH:MeMhSdxL2oAfd3rRXRJ6TH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....S.....0..1.....Q... ..`....@.. .....x... .@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x51519f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x53871FEE [Thu May 29 11:54:22 2014 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x115084	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x116000	0x3d4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x118000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1150ce	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1131a5	0x113200	False	0.837859566674	data	7.39943250791	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x116000	0x3d4	0x400	False	0.392578125	data	3.09213613055	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x118000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x116058	0x37c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	Hospital_project.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	WindowsFormsApplication1
ProductVersion	1.0.0.0
FileDescription	WindowsFormsApplication1
OriginalFilename	Hospital_project.exe

Network Behavior

Snort IDS Alerts

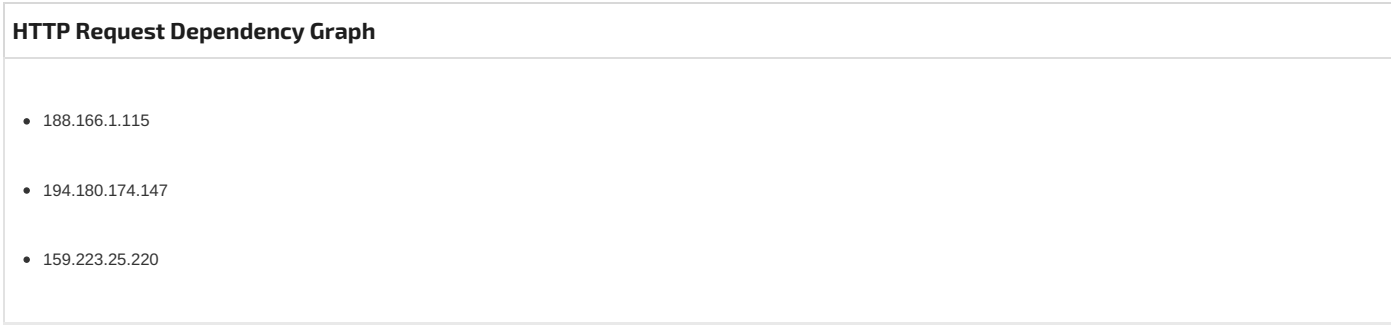
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/29/22-00:12:35.293104	TCP	2034960	ET TROJAN Win32.Raccoon Stealer Checkin M6	80	49814	194.180.174.147	192.168.2.3

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2022 00:11:23.264348030 CET	49742	80	192.168.2.3	188.166.1.115
Jan 29, 2022 00:11:23.294958115 CET	80	49742	188.166.1.115	192.168.2.3
Jan 29, 2022 00:11:23.295171022 CET	49742	80	192.168.2.3	188.166.1.115
Jan 29, 2022 00:11:23.297174931 CET	49742	80	192.168.2.3	188.166.1.115
Jan 29, 2022 00:11:23.325984955 CET	80	49742	188.166.1.115	192.168.2.3
Jan 29, 2022 00:11:55.059446096 CET	49742	80	192.168.2.3	188.166.1.115
Jan 29, 2022 00:11:55.220033884 CET	49745	80	192.168.2.3	188.166.1.115
Jan 29, 2022 00:11:55.250454903 CET	80	49745	188.166.1.115	192.168.2.3
Jan 29, 2022 00:11:55.253822088 CET	49745	80	192.168.2.3	188.166.1.115
Jan 29, 2022 00:11:55.254281998 CET	49745	80	192.168.2.3	188.166.1.115
Jan 29, 2022 00:11:55.283435106 CET	80	49745	188.166.1.115	192.168.2.3
Jan 29, 2022 00:12:27.063874006 CET	49745	80	192.168.2.3	188.166.1.115
Jan 29, 2022 00:12:27.067521095 CET	49789	80	192.168.2.3	91.219.236.139
Jan 29, 2022 00:12:30.077579975 CET	49789	80	192.168.2.3	91.219.236.139

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2022 00:12:31.222625017 CET	49799	80	192.168.2.3	91.219.236.139
Jan 29, 2022 00:12:34.218528032 CET	49799	80	192.168.2.3	91.219.236.139
Jan 29, 2022 00:12:35.065468073 CET	49814	80	192.168.2.3	194.180.174.147
Jan 29, 2022 00:12:35.113210917 CET	80	49814	194.180.174.147	192.168.2.3
Jan 29, 2022 00:12:35.115226030 CET	49814	80	192.168.2.3	194.180.174.147
Jan 29, 2022 00:12:35.115562916 CET	49814	80	192.168.2.3	194.180.174.147
Jan 29, 2022 00:12:35.163053036 CET	80	49814	194.180.174.147	192.168.2.3
Jan 29, 2022 00:12:35.293103933 CET	80	49814	194.180.174.147	192.168.2.3
Jan 29, 2022 00:12:35.293160915 CET	80	49814	194.180.174.147	192.168.2.3
Jan 29, 2022 00:12:35.293205023 CET	80	49814	194.180.174.147	192.168.2.3
Jan 29, 2022 00:12:35.293241978 CET	80	49814	194.180.174.147	192.168.2.3
Jan 29, 2022 00:12:35.293246031 CET	49814	80	192.168.2.3	194.180.174.147
Jan 29, 2022 00:12:35.293272018 CET	80	49814	194.180.174.147	192.168.2.3
Jan 29, 2022 00:12:35.293308020 CET	49814	80	192.168.2.3	194.180.174.147
Jan 29, 2022 00:12:35.298744917 CET	49815	80	192.168.2.3	159.223.25.220
Jan 29, 2022 00:12:35.328320026 CET	80	49815	159.223.25.220	192.168.2.3
Jan 29, 2022 00:12:35.328432083 CET	49815	80	192.168.2.3	159.223.25.220
Jan 29, 2022 00:12:35.328999996 CET	49815	80	192.168.2.3	159.223.25.220
Jan 29, 2022 00:12:35.329063892 CET	49815	80	192.168.2.3	159.223.25.220
Jan 29, 2022 00:12:35.343663931 CET	49814	80	192.168.2.3	194.180.174.147
Jan 29, 2022 00:12:35.358330965 CET	80	49815	159.223.25.220	192.168.2.3
Jan 29, 2022 00:12:35.358364105 CET	80	49815	159.223.25.220	192.168.2.3
Jan 29, 2022 00:12:35.528899908 CET	80	49815	159.223.25.220	192.168.2.3
Jan 29, 2022 00:12:35.578156948 CET	49815	80	192.168.2.3	159.223.25.220
Jan 29, 2022 00:12:53.544519901 CET	49814	80	192.168.2.3	194.180.174.147
Jan 29, 2022 00:12:53.544562101 CET	49815	80	192.168.2.3	159.223.25.220

HTTP Request Dependency Graph



HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49742	188.166.1.115	80	C:\Windows\SysWOW64\LaunchWinApp.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2022 00:11:23.297174931 CET	823	OUT	GET /hdm3prapor HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: text/plain; charset=UTF-8 Host: 188.166.1.115

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49745	188.166.1.115	80	C:\Windows\SysWOW64\LaunchWinApp.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2022 00:11:55.254281998 CET	846	OUT	GET /hdm3prapor HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: text/plain; charset=UTF-8 Host: 188.166.1.115

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49814	194.180.174.147	80	C:\Windows\SysWOW64\LaunchWinApp.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2022 00:12:35.115562916 CET	9750	OUT	GET /hdm3prapor HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: text/plain; charset=UTF-8 Host: 194.180.174.147
Jan 29, 2022 00:12:35.293103933 CET	9752	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 28 Jan 2022 23:12:35 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: stel_ssid=211f13d22189c86382_14521355821524036754; expires=Sat, 29 Jan 2022 23:12:35 GMT; path=/; samesite=None; secure; HttpOnly Pragma: no-cache Cache-control: no-store Strict-Transport-Security: max-age=35768000 Access-Control-Allow-Origin: * Data Raw: 31 31 39 65 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 54 65 6c 65 67 72 61 6d 3a 20 43 6f 6e 74 61 63 74 20 40 68 64 6d 33 70 72 61 70 6f 72 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 68 64 6d 33 70 72 61 70 6f 72 22 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 69 6d 61 67 65 22 20 63 6f 6e 74 65 6e 74 3d 22 68 74 74 70 73 3a 2f 2f 74 65 6c 65 67 72 61 6d 2e 6f 72 67 2f 69 6d 67 2f 74 5f 6c 6f 67 6f 2e 70 6e 67 22 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 73 69 74 65 5f 6e 61 6d 65 22 20 63 6f 6e 74 65 6e 74 3d 22 54 65 6c 65 67 72 61 6d 22 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 61 31 39 32 31 59 6c 63 35 6d 45 56 36 36 66 4b 61 66 79 61 6a 66 35 56 2b 38 30 55 56 38 74 4e 56 76 41 3d 3d 33 64 2d 76 33 35 22 3e 0a 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 74 77 69 74 74 65 72 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 68 64 6d 33 70 72 61 70 6f 72 22 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 74 77 69 74 74 65 72 3a 69 6d 61 67 65 22 20 63 6f 6e 74 65 6e 74 3d 22 68 74 74 70 73 3a 2f 2f 74 65 6c 65 67 72 61 6d 2e 6f 72 67 2f 69 6d 67 2f 74 5f 6c 6f 67 6f 2e 70 6e 67 22 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 74 77 69 74 74 65 72 3a 73 69 74 65 22 20 63 6f 6e 74 65 6e 74 3d 22 40 54 65 6c 65 67 72 61 6d 22 3e 0a 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 61 6c 3a 69 6f 73 3a 61 70 70 5f 73 74 6f 72 65 5f 69 64 22 20 63 6f 6e 74 65 6e 74 3d 22 36 38 36 34 34 39 38 30 37 22 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 61 6c 3a 69 6f 73 3a 61 70 70 5f 6e 61 6d 65 22 20 63 6f 6e 74 65 6e 74 3d 22 54 65 6c 65 67 72 61 6d 20 4d 65 73 73 65 6e 67 65 72 22 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 61 6c 3a 69 6f 73 3a 75 72 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 74 67 3a 2f 2f 72 65 73 6f 6c 76 65 3f 64 6f 6d 61 69 6e 3d 68 64 6d 33 70 72 61 70 6f 72 22 3e 0a 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 61 6c 3a 61 6e 64 72 6f 69 64 3a 75 72 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 74 67 3a 2f 2f 72 65 73 6f 6c 76 65 3f 64 6f 6d 61 69 6e 3d 68 64 6d 33 70 72 61 70 6f 72 22 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 Data Ascii: 119e<!DOCTYPE html><html> <head> <meta charset="utf-8"> <title>Telegram: Contact @hdm3prapor</title> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta property="og:title" content="hdm3prapor"><meta property="og:image" content="https://telegram.org/img/t_logo.png"><meta property="og:site_name" content="Telegram"><meta property="og:description" content="a1921Ylc5mEV66fKafyajf5V+80UV8tNVvA==3d-v35"><meta property="twitter:title" content="hdm3prapor"><meta property="twitter:image" content="https://telegram.org/img/t_logo.png"><meta property="twitter:site" content="@Telegram"><meta property="al:ios:app_store_id" content="686449807"><meta property="al:ios:app_name" content="Telegram Messenger"><meta property="al:ios:url" content="tg://resolve?domain=hdm3prapor"><meta property="al:android:url" content="tg://resolve?domain=hdm3prapor"><meta prop

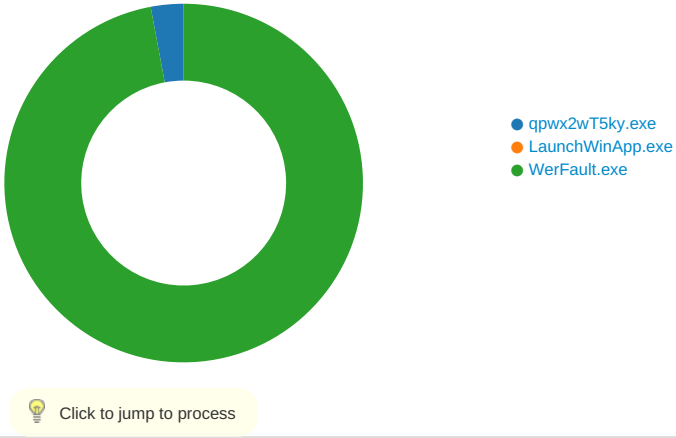
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49815	159.223.25.220	80	C:\Windows\SysWOW64\LaunchWinApp.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2022 00:12:35.328999996 CET	9756	OUT	POST / HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: text/plain; charset=UTF-8 Content-Length: 128 Host: 159.223.25.220

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2022 00:12:35.528899908 CET	9757	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 28 Jan 2022 23:12:35 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 61 32 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: a2<html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx </body></html>0

Statistics

Behavior



System Behavior

Analysis Process: qpwx2wT5ky.exe PID: **6428**, Parent PID: **2016**

General	
Target ID:	0
Start time:	00:12:08
Start date:	29/01/2022
Path:	C:\Users\user\Desktop\qpwx2wT5ky.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\qpwx2wT5ky.exe"
Imagebase:	0xd10000
File size:	1128960 bytes
MD5 hash:	C22C0FDBC19DCD4838709BBACA921F56
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000002.318536230.0000000004271000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000000.00000002.318536230.0000000004271000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000003.301171439.0000000004615000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000003.301171439.0000000004615000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000000.00000002.320185486.000000000468C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.317108118.0000000003170000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000002.317108118.0000000003170000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_DisableWinDefender, Description: Detects executables containing artifcats associated with disabling Widnows Defender, Source: 00000000.00000002.317108118.0000000003170000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCMD, Description: Detects Windows exceutables bypassing UAC using CMSTP utility, command line and INF, Source: 00000000.00000002.317108118.0000000003170000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: 00000000.00000002.317108118.0000000003170000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste, Description: Detects executables potentially checking for WinJail sandbox window, Source: 00000000.00000002.317108118.0000000003170000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000003.301603484.0000000005962000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000003.301092646.000000000452D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000003.301092646.000000000452D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\qpwx2wT5ky.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E95C78D	CreateFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\qpwx2wT5ky.exe	C:\Users\user\AppData\Local\Temp\8a5117119915447493a5b09e32efc8ff.tmp	success or wait	1	6AA446F	MoveFileExA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\qpwx2wT5ky.exe.log	0	617	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6E95C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E62CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5803DE	ReadFile
C:\Windows\SysWOW64\LaunchWinApp.exe	unknown	33280	success or wait	1	6C3A1B4F	ReadFile

Analysis Process: LaunchWinApp.exe PID: **5980**, Parent PID: **6428**

General

Target ID:	2
Start time:	00:12:13
Start date:	29/01/2022
Path:	C:\Windows\SysWOW64\LaunchWinApp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\LaunchWinApp.exe
Imagebase:	0xa0000
File size:	33280 bytes
MD5 hash:	529B7E6E938EA6C3BCA2821EB525BBD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000002.00000000.308435428.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Raccoon, Description: Raccoon stealer payload, Source: 00000002.00000000.308435428.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000002.00000002.503612673.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Raccoon, Description: Raccoon stealer payload, Source: 00000002.00000002.503612673.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000002.00000000.308711684.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Raccoon, Description: Raccoon stealer payload, Source: 00000002.00000000.308711684.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000002.00000000.309062654.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Raccoon, Description: Raccoon stealer payload, Source: 00000002.00000000.309062654.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000002.00000000.308140277.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Raccoon, Description: Raccoon stealer payload, Source: 00000002.00000000.308140277.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000002.00000000.467738406.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Raccoon, Description: Raccoon stealer payload, Source: 00000002.00000000.467738406.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000002.00000000.309415722.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Raccoon, Description: Raccoon stealer payload, Source: 00000002.00000000.309415722.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000002.00000000.467293779.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Raccoon, Description: Raccoon stealer payload, Source: 00000002.00000000.467293779.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	low

Analysis Process: WerFault.exe PID: **5952**, Parent PID: **5980**

General

Target ID:	16
Start time:	00:13:29
Start date:	29/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5980 -s 796
Imagebase:	0x160000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C6.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LaunchWinApp.exe_774587b722d421177778692fbd3ea27ebb729dee_d75afd38_16ec8da7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LaunchWinApp.exe_774587b722d421177778692fbd3ea27ebb729dee_d75afd38_16ec8da7\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F76497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C6.tmp	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C6.tmp.xml	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA0F1.tmp.csv	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA40E.tmp.txt	success or wait	1	6F76497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 31 fd fd 61 fd 05 12 00 00 00 00 00	MDMP 1a	success or wait	1	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	7432	6	00 00 00 00 00 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 08 1d 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 5c 17 00 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT\a0Pacific Standard TimePacific Daylight Time	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	8950	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 74 dd 02 00 00 00 00 74 dd 02 fd 01 00 00 07 00 00 00 01 00 00 00 fd 9d 02 42 34 45 00 23 00 00 00 02 02 00 00 6c 9d 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++ttB4E#l+	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	1632	168	fd 17 00 00 00 00 00 00 09 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 42 34 45 00 00 00 00 00 01 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 22 00 00	B4E"	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	12530	20	1e 00 00 00 fd fd 11 05 00 00 00 00 34 03 00 00 fd 32 00 00	42	success or wait	30	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	13014	820	fd fd 64 77 fd fd 62 77 50 00 00 00 fd fd fd fd 10 00 00 00 60 fd 11 05 2c fd 11 05 fd fd fd fd 40 fd 62 77 40 fd 62 77 fd fd fd fd 00 50 fd 02 00 50 fd 02 fd fd fd 02 50 00 00 00 fd fd fd fd 50 00 00 00 fd fd fd fd 00 50 fd 02 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 38 40 fd 02 00 00 00 00 00 00 00 00 40 1d fd 02 00 00 fd 02 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 02 fd 02 74 fd fd 04 fd 07 fd 02 7c fd fd 04 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	dwbwP`,@bw@bwPPPP P8@@Tt|	success or wait	29	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	48458	4	73 79 6e 74	synt	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	1800	4	04 00 00 00		success or wait	4	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	9666	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 74 dd 02 00 00 00 00 74 dd 02 fd 01 00 00 fd fd fd fd fd fd fd fd 9d 02 42 34 45 00 23 00 00 00 02 02 00 00 6c 9d 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++ttB4E#l+	success or wait	4	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	1948	48	48 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 fd 02 00 00 00 00 fd fd 11 05 00 00 00 00 34 03 00 00 fd 32 00 00 fd 02 00 00 26 2e 00 00	H P42&.	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	2008	4	2b 00 00 00	+	success or wait	43	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	7438	38	20 00 00 00 4c 00 61 00 75 00 6e 00 63 00 68 00 57 00 69 00 6e 00 41 00 70 00 70 00 2e 00 65 00 78 00 65 00 00 00	LaunchWinApp.exe	success or wait	43	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	6548	120	00 00 fd 76 00 00 00 00 00 70 00 00 07 fd 00 00 28 63 3e 35 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 05 00 00 00	vp(c>5!BB? @E	success or wait	5	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	8680	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6OnDemandConnRouteHelper.dll	success or wait	5	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	6764	668	00 00 fd 72 00 00 00 00 00 10 01 00 03 fd 01 00 fd 1f 6d fd fd 22 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fd fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 70 40 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 31 7e 03 00 00 00 00 00 33 7e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 5c 1b 00 00 00 00 00 4a fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 04 05 00 00 00 00 00 26 fd 05 fd 00 00 00 00 fd 63 fd 24 00 00 00 00 fd 96 10 00 00 00 00 6a 2f 45 01 00 00 00 00 fd fd 00 00 79 00 00 fd 05 07 00 fd fd 0a 00 4a fd 04 00 fd 7e 15 00 fd 04 05 00 1d 57 3d 00 fd 3f 01 00 fd fd 18 00 00 00 00 00 17 25 26 00 1b 4d 04	rm"Zbp@1~3~\J@&c$j/EJ~W=?%&M	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	48462	12696	12 00 00 00 44 00 69 00 72 00 65 00 63 00 74 00 6f 00 72 00 79 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72	DirectoryEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer	success or wait	1	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDED.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 28 12 00 00 fd 07 00 00 0e 00 00 00 fd 00 00 00 00 1a 00 00 05 00 00 00 fd 01 00 00 fd 30 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 20 00 00 06 fd 00 00 15 00 00 00 fd 01 00 00 fd 1a 00 00 16 00 00 00 fd 00 00 00 70 1c 00 00	(0`8T p	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5980</Pid>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1002	78	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 4c 00 61 00 75 00 6e 00 63 00 68 00 57 00 69 00 6e 00 41 00 70 00 70 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>LaunchWinApp.exe</ImageName>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1080	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1084	2	09 00		success or wait	2	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1088	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1178	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1182	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1186	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 34 00 38 00 31 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>84810</Uptime>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1230	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1234	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1238	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1320	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1324	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1328	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1380	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1384	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1388	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1432	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1436	2	09 00		success or wait	3	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1442	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 35 00 39 00 30 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>127590400</PeakVirtualSize>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1530	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1534	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1540	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 35 00 38 00 38 00 36 00 30 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123588608</VirtualSize>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1612	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1616	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1622	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 38 00 38 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2881</PageFaultCount>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1696	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1700	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1706	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 34 00 32 00 30 00 38 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>9420800</PeakWorkingSetSize>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1802	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1806	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1812	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 34 00 32 00 30 00 38 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>9420800</WorkingSetSize>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1892	4	0d 00 0a 00		success or wait	1	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1896	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	1902	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 33 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>173952</QuotaPeakPagedPoolUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2016	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2020	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2026	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 33 00 38 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>173832</QuotaPagedPoolUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2124	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2128	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2134	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 36 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>34608</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2258	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2262	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2268	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 33 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>32360</QuotaNonPagedPoolUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2376	4	0d 00 0a 00		success or wait	1	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2380	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2386	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 31 00 36 00 37 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3616768</PagefileUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2462	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2466	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2472	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 38 00 31 00 33 00 33 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3813376</PeakPagefileUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2564	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2568	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2574	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 31 00 36 00 37 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3616768</PrivateUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2646	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2650	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2654	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2700	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2704	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2708	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2738	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2742	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2748	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2788	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2792	2	09 00		success or wait	4	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2800	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6428</Pid>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2830	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2834	2	09 00		success or wait	4	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2842	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>(unable to retrieve)</ImageName>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2928	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2932	2	09 00		success or wait	4	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	2940	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3030	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3034	2	09 00		success or wait	4	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3042	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 39 00 38 00 30 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>89807</Uptime>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3086	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3090	2	09 00		success or wait	4	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3098	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3180	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3184	2	09 00		success or wait	4	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3192	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3244	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3248	2	09 00		success or wait	4	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3256	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3300	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3304	2	09 00		success or wait	5	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3314	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 39 00 31 00 30 00 31 00 32 00 38 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>191012864</PeakVirtualSize>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3402	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3406	2	09 00		success or wait	5	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3416	56	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>0</VirtualSize>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3472	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3476	2	09 00		success or wait	5	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3486	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 30 00 39 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>16091</PageFaultCount>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3562	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3566	2	09 00		success or wait	5	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3576	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 34 00 33 00 39 00 38 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>34398208</PeakWorkingSetSize>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3674	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3678	2	09 00		success or wait	5	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3688	76	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>20480</WorkingSetSize>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3778	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 36 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>286984</QuotaPeakPagedPoolUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3906	88	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>0</QuotaPagedPoolUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3994	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	3998	2	09 00		success or wait	5	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4008	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21664</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4132	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4136	2	09 00		success or wait	5	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4146	100	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>0</QuotaNonPagedPoolUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4246	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4250	2	09 00		success or wait	5	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4260	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4332	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4336	2	09 00		success or wait	5	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4346	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 31 00 38 00 38 00 37 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35188736</PeakPagefileUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4440	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4444	2	09 00		success or wait	5	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4454	68	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>61440</PrivateUsage>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4522	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4526	2	09 00		success or wait	4	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4534	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4580	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4584	2	09 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4590	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4632	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4636	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4640	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4672	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4676	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4678	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4720	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4724	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4726	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4764	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4768	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4772	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	9	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	18	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	4832	82	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 4c 00 61 00 75 00 6e 00 63 00 68 00 57 00 69 00 6e 00 41 00 70 00 70 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>LaunchWinApp.exe</Parameter0>	success or wait	9	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	5538	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	5542	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	5544	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	5584	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	5588	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	5590	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	5628	4	0d 00 0a 00		success or wait	6	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	5632	2	09 00		success or wait	12	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	5636	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6190	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6194	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6196	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6236	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6240	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6242	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6288	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6382	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6386	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6390	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 71 00 72 00 61 00 6c 00 66 00 6e 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>qralfn, Inc.</SystemManufacturer>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6496	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6500	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6504	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 72 00 61 00 6c 00 66 00 6e 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>qralfn7,1</SystemProductName>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6600	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6604	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6608	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.13989454.B64.1906190538</BIOSVersion>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6728	4	0d 00 0a 00		success or wait	1	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6732	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6736	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 39 00 31 00 35 00 32 00 34 00 31 00 30 00 37 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1591524107</OSInstallDate>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6818	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6822	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6826	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6928	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6932	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	6936	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7004	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7008	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7010	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7050	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7054	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7056	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7090	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7094	2	09 00		success or wait	2	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7098	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7194	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7198	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7200	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7236	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7240	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7242	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7266	4	0d 00 0a 00		success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7270	2	09 00		success or wait	6	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7274	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7528	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7532	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7534	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7564	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7566	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 31 00 2d 00 32 00 39 00 54 00 30 00 38 00 3a 00 31 00 33 00 3a 00 33 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-01-29T08:13:38Z">	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7666	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7670	2	09 00		success or wait	2	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7674	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 39 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 39 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 37 00 34 00 33 00 32 00 37 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 37 00 34 00 33 00 32 00 37 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<Process AsId="397" PID="5980" UptimeMS="74327" TimeSinceCreationMS="74327" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7940	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7944	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7948	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7968	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7972	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	7974	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8012	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8016	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8018	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8056	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8060	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8064	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 30 00 39 00 36 00 34 00 30 00 37 00 32 00 2d 00 61 00 39 00 32 00 39 00 2d 00 34 00 34 00 38 00 63 00 2d 00 38 00 61 00 36 00 31 00 2d 00 63 00 64 00 62 00 39 00 38 00 61 00 36 00 34 00 38 00 38 00 63 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>50964072-a929-448c-8a61-cdb98a6488ce</Guid>	success or wait	1	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8162	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8166	2	09 00		success or wait	2	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8170	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 31 00 2d 00 32 00 39 00 54 00 30 00 38 00 3a 00 31 00 33 00 3a 00 33 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-01-29T08:13 :38Z</CreationTime>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8268	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8272	2	09 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8274	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8314	4	0d 00 0a 00		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER118.tmp.WERInternalMetadata.xml	8318	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C6.tmp.xml	0	4768	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LaunchWinApp.exe_774587b722d421177778692fbd3ea27ebb729dee_d75afd38_16ec8da7\Report.wer	0	2	fd fd		success or wait	1	6F76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LaunchWinApp.exe_774587b722d421177778692fbd3ea27ebb729dee_d75afd38_16ec8da7\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	171	6F76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LaunchWinApp.exe_774587b722d421177778692fbd3ea27ebb729dee_d75afd38_16ec8da7\Report.wer	11504	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 32 00 31 00 33 00 36 00 34 00 34 00 39 00 34 00 39 00 34 00	MetadataHash=-2136449494	success or wait	1	6F76497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe\ed89ab84	success or wait	1	6F7836BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F781FB2	RegCreateKeyExW
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F7643D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe\ed89ab84	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe\ed89ab84	FileId	unicode	00000b39e6e098067f0af85d361d5107ab224dc4b1b5	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe\ed89ab84	LowerCaseLongPath	unicode	c:\windows\syswow64\launchwinapp.exe	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe\ed89ab84	LongPathHash	unicode	launchwinapp.exe\ed89ab84	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe\ed89ab84	Name	unicode	launchwinapp.exe	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe\ed89ab84	Publisher	unicode	microsoft corporation	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe\ed89ab84	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe\ed89ab84	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe\ed89ab84	BinaryType	unicode	pe32_i386	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe\ed89ab84	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6F7836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe|ed89ab84	ProductVersion	unicode	10.0.17134.1	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe|ed89ab84	LinkDate	unicode	09/30/2033 12:45:53	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe|ed89ab84	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe|ed89ab84	Size	B	00 82 00 00 00 00 00 00	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe|ed89ab84	Language	dword	1033	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe|ed89ab84	IsPeFile	dword	1	success or wait	1	6F7836BF	unknown
\REGISTRY\A\{a61c5c46-e8fd-436c-3504-8be320ff9699}\Root\InventoryApplicationFile\launchwinapp.exe|ed89ab84	IsOsComponent	dword	1	success or wait	1	6F7836BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 01 00 00 00 00 00 00 00 42 34 45 00 01 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6F781FE8	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly